广播电视监测网网络安全策略

摘　要：广电行业信息化、网络化的快速发展，广电监测从以往零散的单一人工操作变成网络化、智能化以及系统化的现代方式，监测网的创建促使监测工作出现了质的变化，提升了信息反馈速率、丰富了监测数据内容、扩展了监测业务种类、加大了监测地理领域，大幅度提升了广电行业整体监测水平。但是，伴随网络规模的持续拓展，监测网的烦琐性与风险性逐渐加大，业务拓展对网络性能提出了更高要求。怎样采用先进的科技方案，确保监测网络稳定是当前面临的一大问题。

关键词：广电行业；监测网；网络安全；策略分析
中图分类号：TN915.08　　文献标识码：A
文章编号：1671-0134（2019）07-114-03　　DOI：10.19483/j.cnki.11-4653/n.2019.07.037

文 / 魏巾豪

广电监测网属于广电行业中十分核心的基础性任务，监测质量和社会大众的精神文化生活密切联系。随着国内各级广电栏目的逐渐增加、广电网络持续延展，监测网络的服务范围逐渐扩大，就使得监测过程逐渐繁琐化，增多了任务量，给监测网络稳定运行带来巨大风险，且多种广电衍生项目的快速增多，同样对广电网络质量提出了较高要求。为此，广电安全是一个需要高度重视、高度预防警戒的因素。对于广电监测网也是一项需要在质量、安全、监测方面轻视不得的高难度工作。

1. 广电监测网系统分析

监测系统以计算机网络平台、千兆以太网系统、动态路由系统、链路冗余系统等为依据，属于一个集视频、语音及信息于一体的信息传送网络。结合监测网络信息传送量大、时效性高，对信息安全性、稳定性和统一性需求高等特征，在全网络的总体设计阶段，要考量以下几点需求。

（1）配合健全的防火墙系统，制定安全的处理计划，满足保密需求。支撑 AAA 性能、ACL、IPSEC、NAT 、路由检验、CHAP、PAP、CA、MD5、DES、日志等多种功能。

（2）需要网络的物理架构、逻辑架构以及地址空间层次化与模块化，科技及产品规范化，且具备可持续性，有助于网络的建成和拓展；并伴随网络的进步，能持续延展，充分保障现有资源。

（3）系统需要容错性好、防损性能高、稳定性强，网络内单点故障并不会令局域网络丧失于全网络的链接，多点异常不会导致全网络被分为几个互不连接的部分。

（4）满足多业务开展要求，提供高性能的能为图像、语音、信息提供服务的业务网。

（5）通信协议与接口满足国际规定。

（6）结合当前的要求与能够预见的要求增长状况规划网络，不强调空洞的技术科学性，防止追求高档与最新科技而消耗巨大资金。

（7）具备很高的传送宽带，且可以在高负荷条件下依然具备很强的吞吐性能及效率，延迟小。

2. 监测网系统的安全问题

当前，国内广电监测网系统在安全层面存在较大问题，具体表现如下：

2.1 烦琐的系统布局影响安全

国内广电行业最明显的特征即与国内广域国土资源有关，即广电行业的疆域较广，该广度基本已包含中国所有国土的绝大多数区域，甚至已包含中国的一些无人区。与之对应的监测网络平台也持续拓展，导致国内广电监测系统显现地理方面的分散性，在通讯方式方面的烦琐多样性，在节点方面的布局性。正是由于这些性质，导致我国进行全面的、高效的、真正可以保证安全的监控变得非常困难。

因为国内各大广电单位间存在设施和技术的不一致性，部分已发展好的大型省级以及省级电视台已具备能力分布超出中央级的广电设施。而且，各大广电站均能够选用不同的以及多种通讯模式共存的信息传送和传播途径。而每一种信息传送和传播方法及监测的方式方法都有区别，该种烦琐性给监测系统的安全带来了巨大威胁。

分布性，分布性最常见的难点即分布监测系统的也应与之相应的布局，但是分布并非最后目的，最后的目的在于实现即时的集中管理及控制，在一个十分广阔的地区上分布已经很难，得到实时的集中管控便会难之又难。

2.2 IP 网络本身存在的安全问题

世界各地的广电监测系统包含国内广电监测系统，均是一种和互联网结构一样的依靠 TCP/IP 协议的体系。还有依靠无线的和模拟信号的监控网络平台。TCP/IP 网络尽管出现的历史比较久，但该种依靠 TCP/IP 协议的公开性、贯通性、访问性、探测性也是非常容易被攻击的缺点。

2.3 管理制度不完善

广电监测网快速发展，规模及网络出现了巨大扩张，但在系统建立、保障网络平台安全运转及数据保密方面，当前依旧缺乏集中的安全标准、整体的管理制度和法律条文。系统管理不只是对计算机、网络设施、系统软件的控制，还涉及对总体数据资源的管控，对数据资源的标准化、科学化管理。唯有制定科学的安全管理制度，方可令物理层、运用层等安全对策真正高效。

2.4 黑客入侵计算机系统

黑客是威胁网络安全的关键因素，计算机系统内的黑客利用本身所掌握的计算机专业知识来破坏计算机网络平台，是借助计算机系统犯罪的主体。是指利用自己编写或是其他的病毒设施监测网络内的漏洞，然后侵袭网络，黑客的各种行为极大地威胁着计算机系统的安全性。

和单机环境比较，网络平台通信功能高，所以病毒传递迅速，同时提高了测病毒的困难性。从物理角度说，计算机系统的安全比较脆弱，由广电系统内的网络结构图（见图 1）能够发现，广电系统通过制作播报、信号传递、发射配置、客户接收几个网络过程，就像通信方面所遇到的问题那样，计算机网络包含设施分布普遍，任何个人和部门都无法时刻全面监测这些设施，任何设置在无法上锁的地区的设施，包含通讯光缆、电缆、LAN 与电话线、远程网等均有可能受到损坏，进而导致计算机系统瘫痪，阻碍正常信息业务传递。在日常操作中的危害包括：降低计算机和网络系统稳定的运行效率，损坏计算机操作平台和客户的信息，损坏计算机硬件平台，关键数据被盗取等。

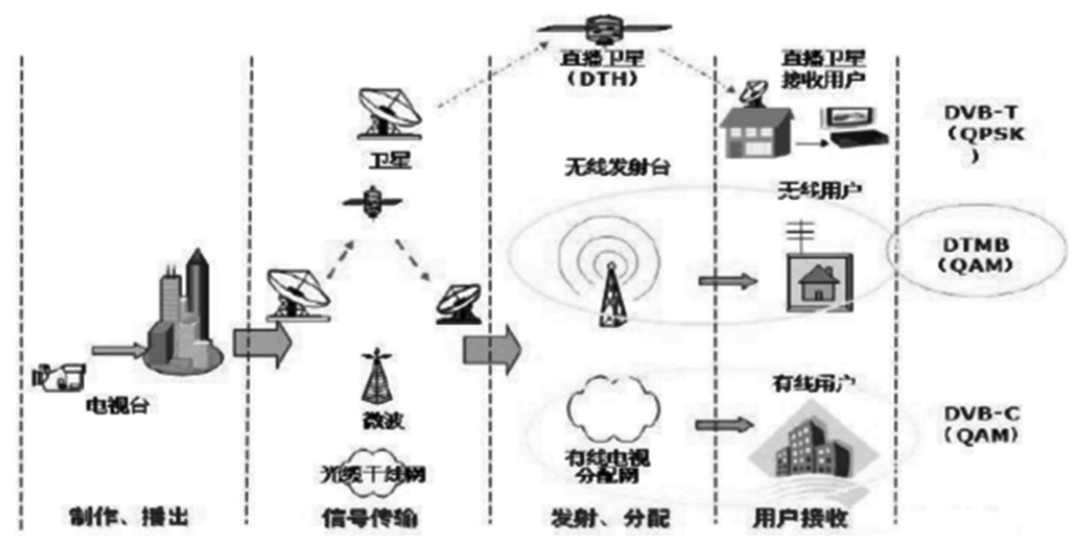


图 1　广电系统内的网络结构

3. 广电监测网安全对策

广电监测网络安全对策要全面考量技术措施与管理措施。从技术层面来讲，因为采用系统的烦琐性，单调的安全对策远无法迎合应用系统的烦琐需求。所以，要求提出多种安全对策，而且与各种应用系统运转在相同网络中一样，网络安全也需要是一个集中、全面的处理计划，需要制定一个层次性安全系统结构。

3.1 操作平台安全对策

操作平台的安全漏洞，大都是因为系统控制不善所引起的。比如，密码设置不善且不定时调整、文件权限设立不当、服务器的搭配不当等，要制定完善的操作平台安全升级体系，立即下载且安装补丁。

3.2 备份对策

为保障监测网络安全可靠运转，针对安全网的重要 LAN 平台硬件，能采取双机热备计划，对运用服务器、信息库服务器、文档服务器、交换器、防火墙等硬件选择双机共行，负载平衡的模式运转，确保任何一点产生问题，系统均可以智能切换至热备硬件上工作，不影响系统稳定应用。但是，以上方案需要投入巨大资金，在经费有限的情况下也能采取热备份计划，但需要定时的人工备份与维护检测，方可在产生故障时减少处理时间。

3.3 网络资源设计对策

创建监测网以前，要统一规划网络资源，建立科学的 IP 计划、网络拓扑计划，对多种资源实现集中编码，创建集中的信息字典。实践表明，科学的、集中的网络计划对网络维护和安全运转均有较大优势，有助于保证网络在持续拓展中的长远性与可靠性，持续克服与处理产生的技术故障。

3.4 设施安全配备方法

针对核心网络设施，如交换器、路由器等要求建立科学的配备管理方法，闭合不重要的设施服务，采用强口令和密码，增强设施访问认证及授权，创新 BIOS，采用访问管理列表权限、制约信息包类别等。

3.5 防病毒对策

病毒属于网络安全中常见的隐患，因为其传递迅速、破坏力强等特征，持续威胁着所有网络安全。就体系结构层面来说，监测网平台具有点多面广的特征，防毒平台应当是多角度、多层次的。[1] 采取统一管理、多层次防护方法，能在监测网每个网络均分级设置防病毒软件，核心网络对下级平台要实施统一病毒监控，定期升级。管理控制阶段，制定与采取集中的防病毒对策，如此既能够降低管理者的工作压力，还可以保证整个网络内每台计算机涉及服务器与用户端具备相同且强大的防病毒性能。

3.6 网络安全对策

首先，防火墙平台。监测网因其布局限制，通常由诸多安全域构成，要加防火墙，封闭核心端口，对各个安全边界采取访问管理，对来往工作记录日志。借助防火墙得到系统中各级网络间的分隔与访问控制，并对公开服务设备的安全防护与对远程客户的安全认证及 ACL，而且可以实现对专线信息的流量控制及管理与防入侵。防火墙作用准确实施的核心是其安全对策的分配及控制。针对仅有一个 LAN 平台的监测网，防火墙安装与网络进口点检测网络通讯，针对多个 LAN 的分布式监

测平台，防火墙能结合其网络分级设置、统一控制。

其次，LDS。LDS平台是一种全新的网络安全系统，可以补充防火墙的问题，有效处理源于网络中的攻击，可以有效保护网络。[2] 针对分级控制平台，能在每个LAN防火墙之后安装LDS平台，成为分布式布局，各区域对网络流量展开信息分析，当出现异常行为时，记下证据，且向网络控制者报警，而且呈现在各地分中心及总监控中心，统一分析网络行为，并集中采取科学的防范方法。

最后，漏洞扫描。安全漏洞扫描平台是当前最科学的系统，安全评定科技可以定期和不定时的扫描监控网络与多种平台，并向安全控制者提供科学的系统漏洞信息，使管理者可以及时掌握系统目前存在的漏洞，采用科学的措施加以修补。

另外，网络管理对策。网络安全防护的主体由人建立、由人应用、由人管控。而网络侵袭的发起对象也是人，因此网络安全的关键在于人，对网络安全必须加强管理，仅依靠简单的技术工具远远无法达到安全目的，检查一个内部网的安全性既要检查其技术手段，还要检查该网络所选择的各种方法的整体性。

3.7 信息传送安全对策

监测网是一个广域网，无专门的通讯网络，大都借助广电光缆和电信线路实现通讯，信息在广域网中的传递要采用加密方法。[3] 因为传送形式的多元化，在不同状态下的加密方法也不一样。如借助VPN系统和动态加密系统等，要对不同通讯模式及信息的安全级别建立不同的信息传送对策。

3.8 系统安全对策

所有的安全产品均只服务于安全的某个环节，均有一定的局限性，网络属于一个多样、烦琐、动态的平台，无一种安全产品及技术可以迎合网络安全的全部需求。防火墙平台针对内部的侵袭行为与伪装成合法要求的行为是不能预防的，入侵监控与漏洞扫描常常产生误报与漏报。[4] 而且，简单的把诸多安全设施堆砌起来，无法提升网络平台的安全水平。网络安全属于一个多环节的结合，如当IDS平台发现网络不良行为时，能和防火墙、关键保护实现联动；如果防病毒平台找到新病毒时，也要立即更新IDS平台的病毒攻击库，提升IDS平台的工作效率。唯有网络安全的每个构件有效联动、相互补充，方可保证网络安全[5]。而且，业务系统自身处于发展阶段，安全策略也要随着系统的调整而变化，如此方可保证系统的安全策略科学。

3.9 身份认证策略

首先，以口令为主的身份认证模式。针对以往的认证技术而言，其所采取的是以口令为主的认证方式。该种方式较为简单，针对封闭小型平台而言，其是一个简单有效的科学办法，但是客户在筛选口令时，通常均是姓名以及生日，该种口令极易遭到破解，如此一来就存在较大的安全威胁。

其次，以物理证件为主的认证形式。该种形式通过客户的某些特殊东西来实现，所采用的物理证件包括智能卡和USB key等，借助智能卡可以加密硬件系统，其安全程度很高。以智能卡为主的认证形式，将客户所知和客户所有两类形式相融合，在物理证件内存入客户资料，把客户事先加以选取的某一随机信息存进AS内，客户在对系统资源加以访问时，在录入ID和口令以后，系统先判定智能卡的规范性，再借助智能卡判断客户身份，如果客户身份属于合法，随后把智能卡内所存储的随机信息传送致AS实现深入认证。

最后，一次性口令认证方法。一次性口令是指把身份代码和某种无法确定的因素作为密码算法录入参数。借助算法的变换获得一个改变结果，而且将这一结果作为客户完成登录的口令，于认证服务设备端借助与之一样的计算方式进行计算，而且要将之和客户登录口令配合，若是合法的则可登录，该种一次性口令并不重复，而且是持续改变的。此外，客户无需记住，一个口令仅有一次应用权利，属于拒绝反复应用的。就当前情况而言，一次性口令认证方法获得实现的途径主要包括3种：（1）Lamport形式。该种形式也称为哈希链模式，该种计划的实现比较容易，而且无需特殊硬件支撑。但其安全性是基于单向散列函数得以实现，尽量避免在分布式网络条件下应用。（2）时间同步形式。该种形式下，每个客户均有一个相关时间同步令牌。该种形式的核心即要确保认证服务器和令牌时钟的相同。（3）挑战应答形式。该种形式下，所有客户应保持相关挑战应答令牌，而且在令牌中放入有种子密钥和加密算法。客户在访问系统时，将有一个挑战信息与服务器内随机形成，而且将这一信息向客户传送，客户将接收的信息输进令牌中，令牌结合内部加密算法与种子密钥应与之相关应答信息计算出来。客户将这一应答信息向服务器传送，服务器再把相关应答信息计算出来，将之和客户上传信息相对比，进而加以验证。

结语

综上所述，伴随计算机以及相关科技的进步，监测系统的安全性要维持动态运转概念，从而定时检查与评价、持续升级系统与安装补丁、追踪最新的安全风险、结合业务的进展改造系统，创新技术、调整更高质量的产品，或是经过拓扑补偿对安全性能的持续拓展与延续，以确保系统的稳定运转。网络控制在网络建造与维护方面是十分关键的，唯有制定与执行健全的安全控制标准，保证防患于未然，方可保证监测网络安全工作。媒

参考文献

[1] 贾万才．无线广播电视监测网及安全策略[J].黑龙江科技信息,2014(03):37.

[2] 胡茂贵．关于安徽广播电视监测网网络安全的研究[J].网络安全技术与应用,2013(08):126-127.

[3] 李涛．广播电视监测网网络安全研究[J].中国新通信,2013,15(04):33.

[4] 陈宇凤．无线广播电视监测网及安全策略[J].黑龙江科技信息,2011(24):109.

[5] 李金根．广播电视监测网网络安全研究[J].科技创新导报,2011(24):237.

（作者单位：西宁市广播电视监测中心）